



## INTERNATIONAL CYBERSECURITY AND DIGITAL FORENSICS ACADEMY

**Assignment Title:** Creating virtual machines for malware analysis

**Course Code:** ACI803 Malware Analysis for Cybercrime

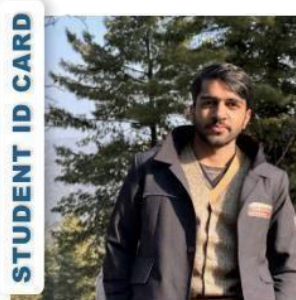
**Student Name:** Ahtisham Tanveer

**Student ID:** 2025/ACI/9979

**Programme:** Advance Cybercrime Investigations

**Instructor Name:** Aminu Idris

**Date of Submission:** 09/14/2025



AHTISHAM TANVEER

2025/ACI/9979

CYBERCRIME INVESTIGATIONS



Exp Date: **November, 2025**

## 1. Introduction

This report documents the setup of a secure malware analysis lab using **Virtual Box** and **FLARE-VM**. The purpose of this setup is to create an isolated environment for safe static and dynamic malware analysis, without exposing the host machine to risk.

The environment follows security best practices:

- Malware samples are handled **only inside the VM**.
- Windows Defender and automatic updates are disabled to avoid interference.
- Snapshots are taken to allow safe rollback if the VM becomes unstable or infected.

## 2. Lab Setup Process

### 2.1 Virtual Box Installation

- Downloaded and installed Virtual Box from [Virtual Box.org](https://www.virtualbox.org).
- Created a new Windows 10 virtual machine with **40 GB disk** and **4 GB RAM**.
- Installed Windows 10 ISO from Microsoft official site.

### 2.2 Guest Additions & Shared Folder

- Installed Virtual Box Guest Additions to enable full-screen mode and clipboard sharing.
- Configured a shared folder for controlled file exchange between host and guest.

### 2.3 System Configuration inside VM

- Disabled **Windows Update** to prevent system changes during analysis.
- Disabled **Windows Defender** (Tamper Protection and real-time monitoring).
- Enabled **Show hidden files** and disabled **hide file extensions** for better visibility of suspicious files.
- Created a **base snapshot** after completing these configurations.

### 2.4 Preparing for FLARE-VM

- Ensured requirements were met: Windows 10, PowerShell v5, internet connectivity, and admin privileges.

### 2.5 Installing FLARE-VM

- Downloaded the FLARE-VM installer script:
- `(New-Object net.webclient).DownloadFile('https://raw.githubusercontent.com/mandiant/flare-vm/main/install.ps1','$([Environment]::GetFolderPath("Desktop"))\install.ps1')`

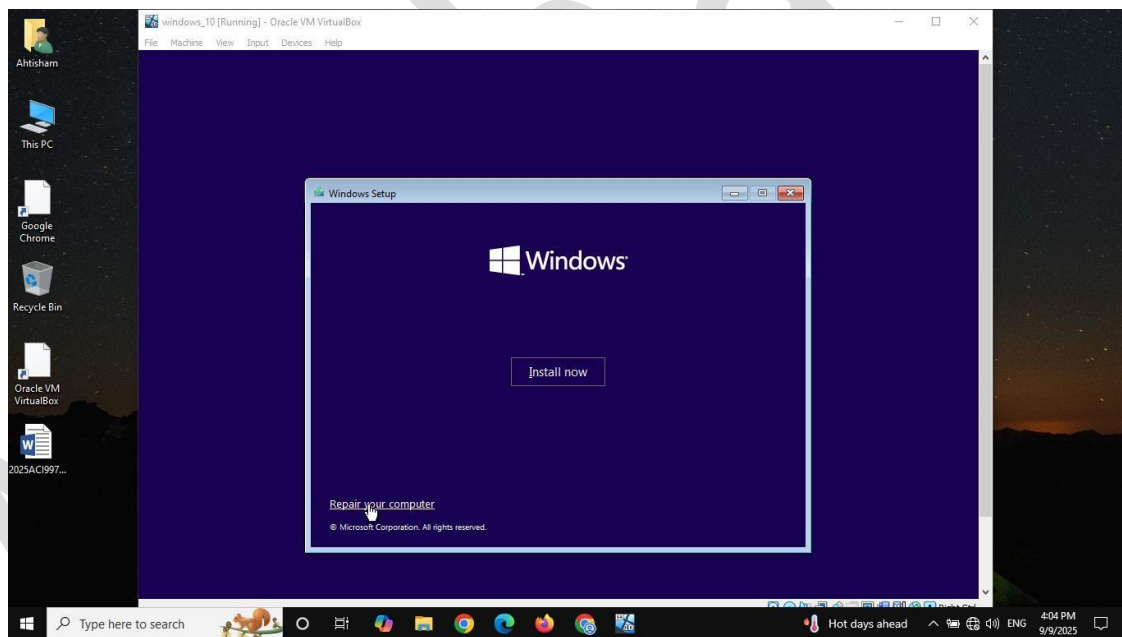
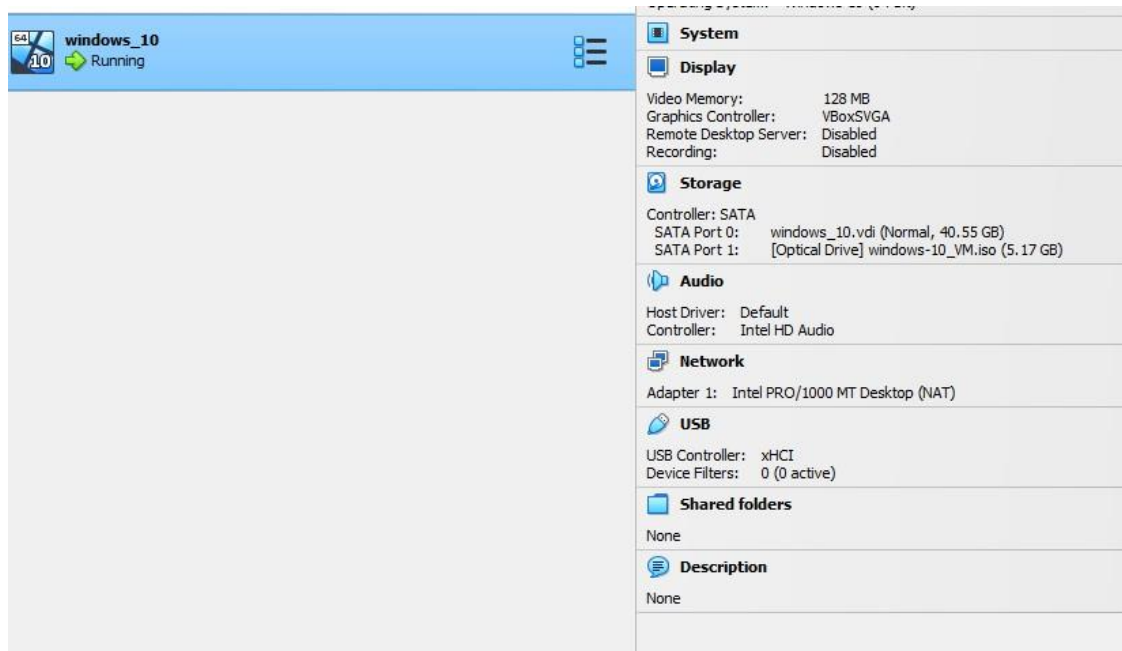
- Unblocked the script:
- Unblock-File .\install.ps1
- Enabled PowerShell script execution:
- Set-ExecutionPolicy Unrestricted -Force
- Executed the installer:
- .\install.ps1
- Installed packages using **Chocolatey** and **Boxstarter**, which automate downloading, configuring, and updating reverse-engineering tools.
- After installation, switched VM to **host-only mode** and took another snapshot.

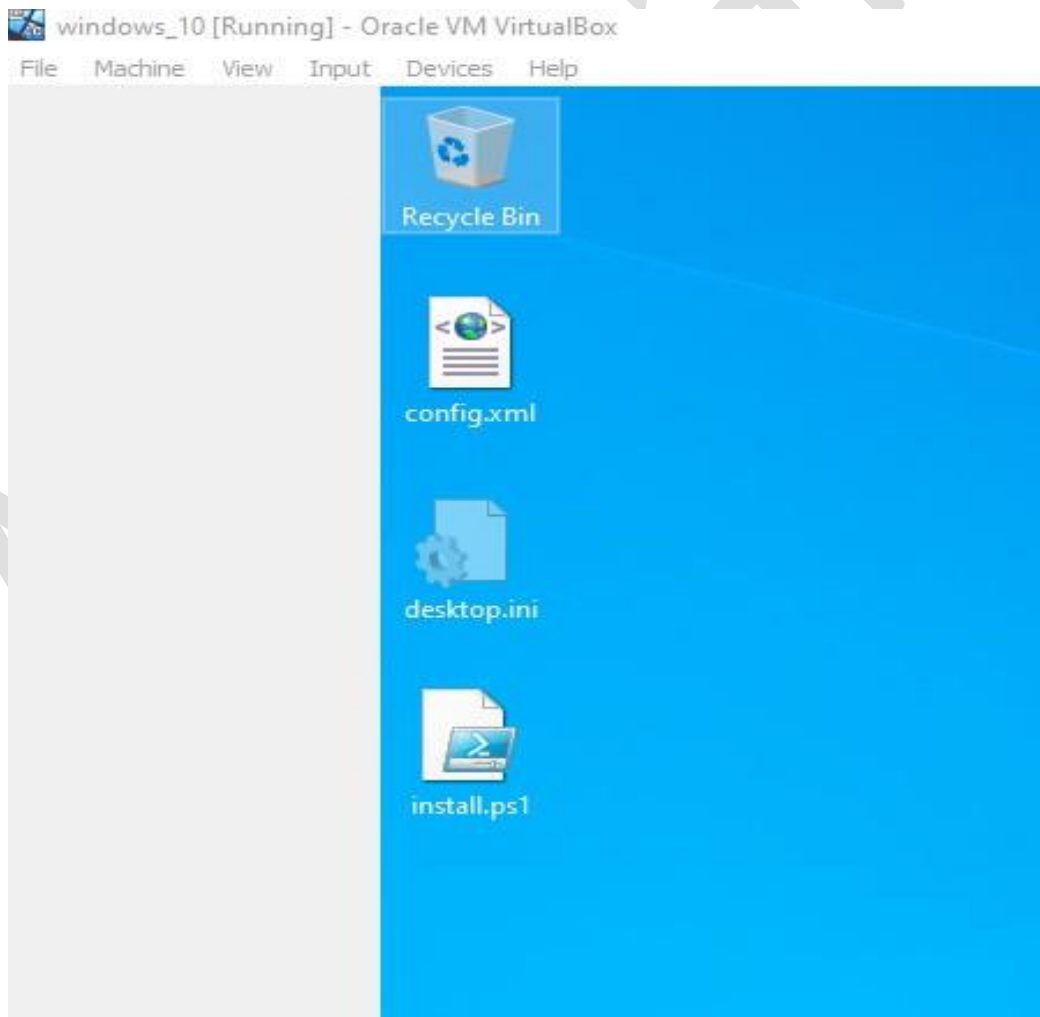
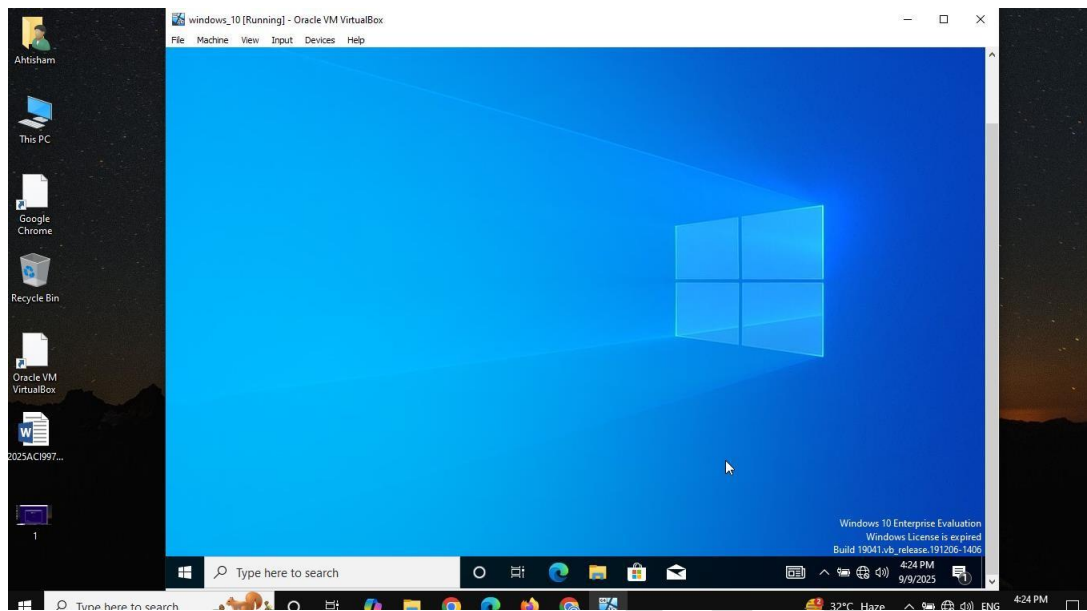
### 3. Challenges and Solutions

Challenge	Resolution
Windows Defender repeatedly quarantined the malware sample	Added Defender exclusions and disabled real-time monitoring during analysis
Script execution blocked in PowerShell	Changed execution policy with Set-ExecutionPolicy Unrestricted
FLARE-VM installation failed due to network issues	Re-ran installer after ensuring internet access and stable connectivity
VM performance slowed during installation	Increased VM memory allocation to 4 GB and enabled virtualization features in BIOS

### 4. Evidence

- Virtual Box VM creation
- Windows 10 running inside VM
- Guest Additions installation
- Disabled Defender & Windows Update
- PowerShell running FLARE-VM installer
- FLARE-VM desktop after successful installation





## Security at a glance

See what's happening with the security and health of your device and take any actions needed.



### Virus & threat protection

Threats found. Start the recommended actions.

Start actions

[See threat details](#)



### Account protection

Sign in with Microsoft for enhanced security and other benefits.

Sign in

[Dismiss](#)



### Firewall & network protection

Firewalls are turned off. Your device may be vulnerable.

Turn on

Windows Security




## Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

### Real-time protection


Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

 Real-time protection is off, leaving your device vulnerable.

☐ Off

### Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

 Cloud-delivered protection is off. Your device may be vulnerable. [Dismiss](#)

☐ Off

## 5. Conclusion

The lab environment was successfully set up using Virtual Box and FLARE-VM.

Key points:

- A **secure, isolated VM** was prepared for malware analysis.
- **FLARE-VM** provided a pre-configured toolkit (Detect It Easy, PEStudio, IDA Free, Ghidra, Strings, etc.).
- **Snapshots** allow safe rollback to a clean state after experiments.
- Challenges with Defender, execution policies, and performance were resolved effectively.

This setup now provides a **stable and safe environment** for performing future malware analysis tasks.